

Check-list de l'acheteur d'une solution de gestion des vulnérabilités (VM)

Les principales questions à vous poser avant de choisir une solution de VM

La gestion des vulnérabilités (VM) correspond à la recherche et à l'élimination systématiques des vulnérabilités présentes sur le réseau. Le choix d'une solution de VM est une étape critique pour protéger le réseau et les données de votre entreprise. Sans une technologie automatisée et éprouvée qui garantit une détection et une remédiation précises, aucun réseau n'est en mesure d'affronter le déluge quotidien de nouvelles vulnérabilités qui menacent la sécurité de votre activité. Pour vous aider à bien choisir la solution à acquérir dans ce domaine, Qualys vous propose une liste de 12 points à prendre en compte pour déterminer l'offre qui correspondra le mieux aux besoins de votre entreprise.

12 repères clés

Architecture

☐ Quel est le mode d'installation de la solution de VM ?

Faut-il installer et maintenir des logiciels ou du matériel ou bien le logiciel est-il fourni sous la forme de service (SaaS) qui nécessite uniquement de se connecter à un compte via un navigateur Web pour lancer l'analyse ? En effet, un système qui vous impose de gérer l'installation, les mises à jour, le matériel, la sécurité de la base de données, etc. finit par coûter plus cher que le prix d'acquisition du logiciel. En outre, ce système peut nécessiter des ressources humaines supplémentaires pour son fonctionnement au quotidien.

☐ La solution a-t-elle une interface utilisateur graphique ?

Certaines offres, plus particulièrement les solutions plus anciennes, d'entrée de gamme ou « sans coût », ne disposent que d'une interface de ligne de commande peu pratique et dont les fonctions de personnalisation (ou contrôles d'accès) sont limitées. Il est important de savoir comment la solution est fournie et de la tester avant de l'acheter.

☐ Dois-je exécuter un agent sur l'ensemble de mes équipements en réseau ?

Les produits logiciels de gestion des vulnérabilités peuvent imposer d'installer et de mettre à jour des agents sur chaque système à analyser. Recherchez donc une architecture qui n'exige ni agent ni un quelconque autre logiciel pour fonctionner, mais seulement un navigateur Web standard en mode SSL pour accéder à l'interface.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Le produit m'oblige-t-il à exécuter une base de données ?

Les produits logiciels de gestion des vulnérabilités peuvent nécessiter d'installer et d'exécuter une base de données pour stocker des informations relatives à la VM. L'architecture SaaS n'impose pas cette contrainte.

☐ Pourquoi m'intéresser à l'offre SaaS pour gérer les vulnérabilités ?

Pour la plupart des entreprises, une solution SaaS est mieux adaptée qu'une offre logicielle pour gérer les vulnérabilités. Cette solution est plus facile à déployer et à gérer. Elle offre davantage de souplesse pour prendre en charge des besoins métier qui évoluent. Elle génère des coûts plus faibles et plus prévisibles. Elle est évolutive et ne vous impose pas une licence sur le long terme. Enfin, elle est plus conviviale et également plus fiable.

Sécurité

☐ Quel est le modèle de sécurité utilisé pour protéger la solution ?

Il est vital que la solution de VM soit elle-même sécurisée, notamment parce qu'elle stocke des données critiques sur les actifs du réseau et sur les vulnérabilités potentielles. Avec des solutions logicielles, sécuriser ces systèmes et les informations associées peut s'avérer une tâche complexe qui vous incombe. À l'aide d'une solution SaaS hébergée, la sécurité est assurée par le fournisseur SaaS. Veillez à ce que la solution SaaS offre une sécurité de bout en bout pour les données de vulnérabilités sensibles. Et aussi à ce qu'elle s'appuie sur de nombreux contrôles proactifs normalisés pour protéger tous les niveaux de l'application.

☐ Comment cette solution est-elle physiquement protégée ?

Insistez sur ce point auprès de votre fournisseur. Au risque de nous répéter, les solutions logicielles traditionnelles vous imposent de faire tout ce travail. A contrario, les solutions SaaS prennent ces points en charge, à votre place. Par exemple, le service QualysGuard est exécuté au sein de centres d'opérations sécurisées (SOC) qui obtiennent chaque année des certifications SAS 70 de Type II. Les machines et les racks QualysGuard sont situés dans une salle machine privée qui impose une authentification par badge et biométrique pour l'accès. L'accès physique est limité à des employés Qualys spécifiques qui subissent des contrôles de référence et de fond effectués par des tiers et qui signent un contrat de confidentialité. Cet accès est sécurisé par un firewall hébergé sur un hôte, par un système de fichiers régi par des politiques et par un système de contrôle d'intégrité, en plus d'une architecture IDS. Le personnel surveille en permanence tous les systèmes et administrent une remédiation et des contre-mesures propres. Le personnel Qualys autorisé à accéder doit être désigné et se prêter à une authentification bifactorielle afin de pouvoir accéder aux serveurs critiques, tous les accès étant consignés dans un journal. Toutes les 24 heures, des sauvegardes complètes sont faites sur un serveur de secours et sur des bandes chiffrées gérées par un tiers pour une rotation hors site.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Comment la solution de VM protège-t-elle la transmission des données de vulnérabilités ?

Si vous choisissez une solution SaaS, assurez-vous que toutes les interactions exigent une connexion HTTPS (SSLv3) avec le tout dernier chiffrement 128 bits AES entre le navigateur Web de l'utilisateur et le système qui effectue les analyses. Soyez très prudents avec les communications en texte clair pour la navigation dans l'interface, le lancement des analyses ou la génération de rapports. Le système doit être capable de prendre en charge les noms d'utilisateur/mots de passe et une authentification à deux facteurs (SecureID) en option pour la connexion. En outre, le mot de passe utilisateur ne doit être stocké sur aucun serveur et le fournisseur de solutions ne doit pas pouvoir accéder à ces mots de passe.

☐ Quels contrôles d'accès sont intégrés à la solution ?

Vérifiez que la solution de gestion des vulnérabilités fournit bien un contrôle d'accès hiérarchique déterminé par le profil de l'utilisateur et les niveaux de privilège. Une stratégie basée sur les meilleures pratiques fournit un contrôle d'accès à base de profil pour cinq profils bien distincts : Manager (contrôle complet), Responsable d'une unité (contrôle sur l'entité), Scanner (autorisé à effectuer des analyses sur des actifs autorisés par le Responsable d'une unité ou le Manager), Lecteur (uniquement autorisé à créer des rapports), et Contact (aucun accès au système, uniquement des alertes par email). Chaque profil doit autoriser des paramètres de configuration supplémentaires pour des permissions granulaires.

☐ Comment la solution de VM protège-t-elle les données d'analyse des vulnérabilités ?

Exigez que les données de vulnérabilités soient chiffrées et stockées en toute sécurité dans une « instance » différente d'une base de données sécurisée. L'algorithme de chiffrement, la clé et le processus de déverrouillage doivent être puissants. Ils ne doivent jamais être enregistrés sur le disque en texte clair ni stockés nulle part ailleurs que temporairement dans la mémoire système lors de la phase d'authentification/de déchiffrement pendant la connexion.

Évolutivité/Convivialité

☐ Qu'est-ce qu'une solution de VM évolutive ?

Lorsque vous utilisez un produit logiciel, son évolutivité est tributaire de l'infrastructure que vous achetez, exploitez et maintenez pour faire fonctionner le produit. Assurez-vous que vous comprenez bien toutes les restrictions de cette offre. Une solution SaaS ne pose quant à elle aucune limite en termes d'évolutivité. Elle peut faire une découverte sur des réseaux externes et des analyses des vulnérabilités au sein des plus grands environnements de réseau d'entreprise. Vous devez pouvoir analyser tous les équipements dotés d'une adresse IP, et ce quotidiennement.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Comment la solution de VM s'adapte-t-elle à la taille de mon réseau ?

Le traitement efficace d'une découverte réseau et d'une analyse des vulnérabilités à grande échelle n'est pas réalisable sans une analyse intelligente. Assurez-vous que le système offre une fonction d'analyse intelligente pour corréler la carte qu'il crée de vos équipements réseau et de leur système d'exploitation, avec toutes les vulnérabilités connues qui affectent chacun des systèmes. Ceci garantit une vitesse et une qualité optimales pour évaluer les vulnérabilités sur votre réseau tout en réduisant au minimum le trafic réseau/hôte.

☐ La solution de VM est-elle totalement automatisée ?

La découverte manuelle (ou mappage) et l'analyse étant des tâches fastidieuses, leur automatisation est un avantage indéniable. Aussi, retenez une solution qui vous permet, d'une part, d'évaluer automatiquement et à tout moment les risques de sécurité sur l'ensemble de votre réseau et, d'autre part, de mesurer immédiatement votre conformité aux normes et aux contrôles externes. Les produits de gestion des vulnérabilités qui nécessitent trop d'intervention manuelle sont une source d'erreurs humaines et de résultats inexacts ainsi qu'une perte de temps et de ressources.

☐ Quel est le niveau de support fourni par la solution ?

Les problèmes de vulnérabilités sont permanents. Aussi, assurez-vous que la solution que vous choisirez intègre bien un support disponible 24 heures sur 24, 7 jours sur 7 et 365 jours par an. Ce support doit comprendre les appels téléphoniques, les courriers électroniques ainsi qu'une documentation en ligne complète, des notes techniques et une foire aux questions. Veillez aussi à ce que le fournisseur puisse répondre aux demandes de support d'après des accords de niveau de service (SLA).

☐ La formation est-elle comprise dans le support ?

Assurez-vous que votre solution de gestion des vulnérabilités vous informe sur tout ce que vous devez savoir et qu'elle offre des programmes de formation et de certifications en direct et enregistrés. Dans l'idéal, ces prestations doivent être incluses dans votre abonnement.

☐ Comment la solution s'intègre-t-elle à d'autres applications ?

L'interopérabilité avec vos autres applications de sécurité informatique est essentielle. La solution de VM doit faciliter un workflow intégré et sur mesure pour l'analyse et la remédiation avec les systèmes existants de centre d'appel/Help Desk tels que Remedy AR System, les principales solutions SIM/SEM telles que Symantec SESA V2, les systèmes de gestion des patches tels que McAfee Remediation Manager, et Cisco Security Monitoring, Analysis, and Response System.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

Précision/Performances

☐ Quel est le degré de précision de la solution de VM ?

Si la solution vient à manquer une vulnérabilité utilisée par les pirates pour compromettre votre réseau, c'est qu'elle n'est « pas assez précise. » Si la solution signale de manière inexacte des problèmes qui ne sont pas réels (c'est-à-dire des fausses alertes), elle va vous inonder de données erronées et vous faire perdre un temps précieux. De nombreux fournisseurs revendiquent un niveau de précision supérieur. Demandez-leur d'étayer leurs déclarations.

☐ D'où provient l'intelligence de la solution de VM en matière de vulnérabilités ?

Votre solution d'analyse doit s'appuyer sur la base de données des vulnérabilités la plus complète du marché et corréler ces informations avec le CERT, DeepSight de Symantec, Security Focus, Secunia, Mitre et Seclists. En outre, la solution doit comprendre des bulletins de sécurité de Microsoft et d'autres éditeurs de logiciels de premier ordre.

☐ Comment la solution actualise-t-elle sa base de données avec les toutes dernières vulnérabilités ?

Avant qu'elles ne soient publiées et rendues publiques (à vous, le client), les signatures de détection des vulnérabilités doivent avoir été testées de manière exhaustive. Souvent, les solutions Open Source n'offrent pas de procédures de test et d'acceptation formelles, ce qui peut vous conduire à utiliser des vérifications inexactes. Qui plus est, les signatures pour les vulnérabilités à haut risque doivent être mises à jour et diffusées dans les heures suivant leur publication. Veillez à ce que le fournisseur dispose d'une base de connaissances crédible et actualisée plusieurs fois par jour avec des vérifications des nouvelles vulnérabilités et des améliorations apportées aux signatures existantes. Il est indispensable que l'ensemble du processus de mise à jour soit totalement automatisé et complètement transparent pour vous (le client).

☐ Mes politiques d'analyse peuvent-elles comprendre automatiquement de nouvelles signatures de vulnérabilités ?

Automatiser les mises à jour de signatures de vulnérabilités est vital. Non seulement pour protéger votre réseau contre les toutes dernières menaces, mais aussi pour garantir l'application permanente des politiques d'analyse de l'entreprise en matière de sécurité. Vérifiez que la solution gère ce processus sans intervention humaine.

☐ Comment la solution de VM affiche-t-elle les vulnérabilités ?

Vous souhaitez légitimement être informés des nouvelles vulnérabilités qui peuvent frapper votre réseau. La solution doit donc afficher une liste des vulnérabilités les plus récentes qui ont été ajoutées à la base de connaissances. Les informations relatives à chaque vulnérabilité doivent comprendre une description détaillée ainsi que des moyens de remédiation. Dans l'idéal, la liste doit être interactive et permettre aux utilisateurs d'interroger à l'aide d'un identifiant CVE, d'un mot clé, de sa fonction, d'une référence fournisseur, etc.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

Découverte/Mappage

☐ La découverte/le mappage est-il un composant de la solution ?

Le processus d'analyse d'un réseau pour y rechercher des vulnérabilités impose de savoir par avance sur quoi les traquer. Les vulnérabilités sont spécifiques et non pas générales. Elles affectent une plate-forme spécifique, un système d'exploitation et un Service Pack, une application et un numéro de version, une version de patch, etc. Assurez-vous que la solution est capable de mapper tous les systèmes présents sur votre réseau et qu'elle corrèle ces informations avec les vulnérabilités pour améliorer et accélérer le traitement d'une analyse. Un inventaire précis permet de hiérarchiser le processus de remédiation et garantit la sélection et l'application des bons patches. En outre, le processus de découverte/mappage garantit une couverture complète de tous les équipements présents sur votre réseau.

☐ La solution facilite-t-elle l'identification de tous les équipements sur mon réseau ?

Si elle est réalisée manuellement, cette tâche peut être une corvée. Assurez-vous que la solution que vous choisirez automatise pleinement ce processus. Vous devez pouvoir entrer simplement une adresse IP ou une gamme d'adresses IP pour que le système identifie rapidement tous les équipements installés sur votre réseau.

☐ Quelles sont les informations que le mappage fournit sur le réseau ?

La fonctionnalité de mappage automatisé de la solution doit permettre de découvrir tous les équipements actifs sur le réseau. Une analyse de faible envergure doit identifier avec précision le système d'exploitation de l'équipement ainsi que le type d'équipement (routeur, commutateur, point d'accès, etc.). Dans l'idéal, le processus de découverte fournira également d'autres informations telles que le nom DNS, le nom NetBIOS ainsi que la date de la dernière analyse de l'équipement.

☐ Le système peut-il découvrir des équipements non conformes ?

Votre cartographie du réseau doit indiquer tous les « nouveaux » équipements qui sont « approuvés » ou « non conformes. » Ainsi, vous aurez une vue complète de votre réseau.

☐ La solution peut-elle corréler les données du mappage avec nos différentes entités ?

Les données du mappage ne doivent pas exister dans un « vide technique ». La solution doit permettre de définir l'inventaire réseau en groupes logiques ou entités de l'entreprise, avec des informations granulaires sur le matériel, les logiciels, les applications, les services et les configurations. Les contrôles d'accès permettent à une entité d'exécuter des cartes, des analyses de vulnérabilités ainsi que des rapports uniquement sur ce qu'elle possède. En outre, associer des données mappées avec des entités aide à mieux exploiter les résultats.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

Analyse

☐ Que rechercher en priorité lors d’une analyse de vulnérabilités ?

L’analyse a pour but de détecter et de résoudre les vulnérabilités sur le réseau. Une analyse des vulnérabilités teste l'efficacité des politiques et des contrôles de sécurité sur votre infrastructure. Pour ce faire, elle doit tester et analyser systématiquement les équipements IP, les services et les applications pour y détecter des failles de sécurité connues. Elle doit également fournir un rapport des vulnérabilités réelles découvertes et indiquer ce que vous devez résoudre par ordre de priorité sans compromettre la stabilité des équipements.

☐ Dois-je lancer manuellement chaque analyse ?

En plus du contrôle manuel, la solution doit vous permettre de planifier à l’avance les analyses qui s’exécuteront automatiquement sans intervention humaine.

☐ La solution supporte-t-elle les analyses externes et internes… en centralisant toutes les données et sans fragiliser mon firewall ?

Ces options concernent l’analyse des équipements situés en dehors du firewall, en opposition à la configuration à l’intérieur du firewall. La solution doit fournir une méthodologie fiable pour effectuer une analyse périmétrique d’adresses IP externes. La solution doit appréhender le réseau dans son ensemble et être en mesure de mapper des domaines et d’analyser des adresses IP se trouvant au-delà du firewall. Les équipements concernés par l’analyse interne doivent pouvoir résister aux attaques à l’aide d’un noyau de système d’exploitation endurci, sans exécuter de services en arrière-plan ou exposés sur le réseau. Les équipements internes doivent automatiquement télécharger les mises à jour logicielles et les nouvelles signatures de vulnérabilités et traiter les demandes de tâches, le tout de manière sécurisée et fiable.

☐ La solution peut-elle accélérer sensiblement la vitesse d’analyse ?

Les grandes entreprises peuvent profiter d’une solution de gestion des vulnérabilités qui optimise la vitesse de l’analyse sans surcharger le réseau. Par exemple, QualysGuard utilise une fonctionnalité de parallélisation des analyses qui augmente la vitesse d’analyse jusqu’à la quadrupler tout en garantissant sa précision. Cette fonctionnalité distribue un processus d’analyse vers de nombreuses appliances d’analyse au sein d’un groupe d’actifs spécifique. Après exécution, les résultats sont fournis dans un rapport unique.

☐ Puis-je analyser les réseaux de mes partenaires commerciaux ?

Les processus métier électroniques sont souvent associés aux partenaires de l’entreprise. Malheureusement, les réseaux de ces derniers pouvant être un vecteur pour exploiter des vulnérabilités, il est vital de les analyser tous. Certaines réglementations concernant la conformité à la sécurité exigent des partenaires qu’ils vérifient l’analyse ou que votre entreprise le fasse à leur place. Votre solution doit être assez souple pour vous permettre d’analyser rapidement une quelconque adresse IP ou gamme d’adresses IP sur Internet afin que vous puissiez l’utiliser pour analyser les réseaux de vos partenaires, tout comme le vôtre.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Les « scans authentifiés » sont-ils pris en charge par le scanner ?

La fonctionnalité d’authentification Windows autorise des scans authentifiés pour Windows. Votre solution de gestion des vulnérabilités doit donc prendre pleinement en charge les scans authentifiés pour Windows et pour les systèmes UNIX, Oracle et SNMP. Ainsi, vous pourrez collecter davantage d’informations système sur des hôtes spécifiques et ainsi améliorer le nombre de vulnérabilités détectées par un scanner. Les scans authentifiés sont obligatoires pour les analyses de conformité.

Reporting

☐ Quels types de rapport la solution fournit-elle ?

Le reporting est une fonctionnalité critique d’une solution de gestion des vulnérabilités parce qu’elle permet de guider les efforts de remédiation. Les scanners réseau sont d’une piètre utilité si le reporting ne vous aide pas à atteindre vos objectifs en matière de sécurité et de conformité, dans les délais et dans un souci de rentabilité. La fonctionnalité de reporting doit être à la fois souple et complète. Les composants de reporting doivent intégrer des actifs réseau (adresses IP et/ou groupes d’actifs), des graphes et des tableaux affichant des synthèses globales ainsi que l’état de la sécurité du réseau, des analyses de tendances, des informations détaillées sur les vulnérabilités découvertes ainsi que des options de filtrage et de tri pour obtenir des vues personnalisées des données.

☐ Quels rapports prêts à l’emploi la solution offre-t-elle ?

La solution doit fournir des rapports par défaut qui répondent aux exigences typiques de la plupart des entreprises. Des rapports avec cartes de pointage sont également indispensables. En effet, ils peuvent vous aider à isoler rapidement les vulnérabilités sur un groupe d’actifs (Asset Group Vulnerabilities), les vulnérabilités ignorées (Ignored Vulnerabilities), les vulnérabilités les plus répandues (Most Prevalent Vulnerabilities), les hôtes les plus vulnérables (Most Vulnerable Hosts) et aussi vous fournir un rapport sur les patches. Optez pour des solutions qui comprennent des rapports pour la Direction, techniques, avec une matrice des risques et SANS20. Si vous êtes soumis à des exigences de conformité spécifiques (par exemple Payment Card Industry), demandez s’il existe des rapports préconstruits qui répondent à ces exigences.

☐ Quelles fonctionnalités de reporting basé sur un modèle et personnalisé la solution fournit-elle ?

En plus des rapports par défaut, la solution de gestion des vulnérabilités doit être assez souple pour vous permettre de consulter les données de vulnérabilités de la manière dont vous le souhaitez. Vous devez pouvoir personnaliser le niveau de détail approprié pour différentes audiences. Les options généralement utilisées comprennent le niveau de gravité de la vulnérabilité, l’identifiant typique ou spécifique (ou CVE), le groupe d’actifs (par exemple la géographie, la fonction système, l’emplacement sur le réseau), l’adresse IP, le service ou le port, l’état (par ex. nouveau, actif, fixe, réouvert), ou la catégorie (par ex. associée au Web, base de données, DNS, RPC, SMB, TCP/IP, etc.). De plus, le support de graphiques pour représenter les ensembles de données choisis doit être assuré.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Comment la fonction de reporting de la solution classe-t-elle les vulnérabilités ?

La solution doit affecter des niveaux de gravité qui s'appuient sur des normes de l'industrie telles que CVE et NIST. Les vulnérabilités doivent être repérées pour les différencier au niveau de leur caractère critique. Par exemple : Le Niveau 1 correspond à un gravité minime tandis que le Niveau 2 renvoie à une gravité moyenne, le Niveau 3 à une gravité sérieuse, le Niveau 4 à une gravité critique et le Niveau 5 à une gravité urgente.

☐ La solution peut-elle partager des rapports avec des personnes désignées ?

Afin de réduire la redondance des efforts à produire, la solution doit systématiquement offrir une fonctionnalité de distribution de rapports. Cette fonctionnalité doit intégrer la collaboration et le partage des rapports sur l'état des vulnérabilités. Cherchez des solutions qui intègrent la possibilité de distribuer et de consulter des rapports d'après le profil de l'utilisateur.

☐ Quels sont les formats fournis par la solution pour les applications de rapports externes ?

La solution de gestion des vulnérabilités doit fournir des options de rapports souples pour une utilisation selon les besoins. Elle doit permettre l'exportation des données des rapports d'analyse vers des applications externes aux formats PDF, HTML (compressé), archive Web (MHT, uniquement pour Internet Explorer), CSV et XML.

☐ Existe-t-il une fonctionnalité pour l'analyse des tendances et le reporting différentiel ?

Pour une gestion stratégique des vulnérabilités, la solution doit permettre d'analyser les tendances et de comparer les données des résultats d'analyse dans le temps. Par exemple, les données sur les tendances doivent être présentées pendant un nombre spécifique de jours, de semaines ou de mois. Un rapport différentiel peut présenter les deux dernières détections suite à l'analyse d'un groupe spécifique d'actifs. Pour comparer les résultats dans le temps, il vous faut pouvoir sélectionner et comparer des ensembles d'analyses effectuées à un moment donné.

☐ Y a-t-il des rapports qui facilitent la conformité à PCI, HIPAA, SOX et autres réglementations ?

La conformité peut être un casse-tête majeur pour le service informatique chargé de produire la documentation qui prouve qu'une entreprise a bien déployé les contrôles de sécurité appropriés et efficaces qu'exigent les différentes lois et réglementations du marché. Intéressez-vous à des solutions qui offrent ces fonctionnalités de reporting sur la conformité avec des modèles conviviaux pour vous permettre d'extraire des données sur les vulnérabilités et la configuration de l'hôte et satisfaire ainsi à vos besoins de reporting spécifiques.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ La solution peut-elle fonctionner avec d'autres technologies de gestion des informations de sécurité (SIM) ?

De nombreuses grandes entreprises utilisent déjà des solutions SIM/SEM. Optez pour des solutions qui prennent en charge de nombreuses intégrations associées, notamment ArcSight, Guardednet, NetForensics, Network Intelligence, Open Systems, Symantec SIM 4.0, NetIQ, Cisco MARS/Protego, Intellitactics et eSecurity.

Remédiation

☐ Pourquoi intégrer la remédiation à un scanner de vulnérabilités ?

Découvrir les actifs, analyser les vulnérabilités et faire un reporting sont des éléments critiques de la gestion des vulnérabilités. Cependant, l'objectif final est de résoudre et d'éliminer les vulnérabilités. Vous opterez donc pour une solution qui intègre un système automatisé de suivi par tickets de remédiation. Le système suit automatiquement les modifications des vulnérabilités détectées après leur remédiation pour veiller à ce que le processus de workflow parvienne à une conclusion heureuse.

☐ Comment la solution déploie-t-elle une politique de remédiation ?

Un contrôle des politiques autorisées doit régir tout workflow de remédiation. La solution doit comprendre des menus pour vous permettre de créer sans peine des politiques de remédiation qui déterminent la manière dont les tickets seront créés et à qui ils seront attribués. Assurez-vous que le système autorise des règles et des permissions déterminées par les profils utilisateur.

☐ Le système doit-il planifier la remédiation dans un ordre particulier ?

Résoudre des vulnérabilités par ordre de gravité est une démarche empreinte de bon sens. Cependant, le système doit aussi vous permettre de factoriser le caractère critique d'actifs qui doivent être patchés. La solution a besoin de fonctionnalités intelligentes pour hiérarchiser la remédiation à l'aide de politiques déterminées par des responsables. Les politiques vous permettent de hiérarchiser automatiquement la remédiation en factorisant la gravité de la vulnérabilité par rapport à son impact sur l'activité. C'est-à-dire comment son exploitation affecterait le fonctionnement d'un actif spécifique, d'une entité, voire de l'ensemble de l'entreprise.

☐ Que se passe-t-il lors de la génération d'un ticket ?

Si les tickets d'incident et le workflow font partie de votre solution de gestion des vulnérabilités, assurez-vous que cette dernière peut générer automatiquement un ticket lorsqu'une vulnérabilité est détectée par une analyse. S'appuyant sur une politique prédéterminée, le ticket doit être affecté à une (des) personne(s) désignée(s) pour la remédiation. Le ticket doit être classé en tant qu'« ouvert » tant qu'il 'n'est pas résolu. La classification passe à l'état « fermé » lorsqu'une analyse ultérieure permet de vérifier que la vulnérabilité a bien été supprimée.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ La fonction de génération de tickets de la solution s'intègre-t-elle aux systèmes externes ?

Les services de Help Desk des grandes entreprises utilisent déjà un système de gestion des tickets d'incidents. Aussi, veillez à ce que la solution de gestion des vulnérabilités puisse s'intégrer à des systèmes de gestion des tickets d'incidents tiers via une « API pour tickets » dédiée qui offre une interface de programmation XML pour l'extraction et le traitement des tickets. Par exemple, QualysGuard assure l'intégration au système de Help Desk de Remedy et dispose d'une « API pour tickets » dédiée pour garantir l'intégration à d'autres solutions de tickets d'incident.

☐ Comment la solution gère-t-elle les efforts de remédiation ?

Sur un réseau de grande taille, de nombreux tickets de remédiation sont souvent ouverts à tout moment. Un responsable doit maîtriser la progression et la conformité à la politique de remédiation en lançant un rapport de remédiation. Assurez-vous que votre solution de gestion des vulnérabilités comprend le reporting à la Direction pour les tickets, les tickets par vulnérabilité, les tickets par utilisateur et les tickets par groupe d'actifs. Tant les utilisateurs que les responsables souhaiteront effectuer des analyses de tendances sur les tickets ouverts afin de pouvoir surveiller la progression. De même, mettez-vous en quête de solutions qui vous permettront de recevoir des mises à jour quotidienne des tickets de remédiation par email.

Conformité aux politiques

☐ Pourquoi intégrer la conformité aux politiques à la solution de VM ?

La fonctionnalité de conformité aux politiques associe la gestion des vulnérabilités aux politiques de sécurité de l'entreprise, aux lois et aux réglementations. Cette fonctionnalité vous permet plus particulièrement de renseigner et d'auditer automatiquement la conformité à des auditeurs internes et externes. Vous économisez ainsi du temps, de l'argent et beaucoup d'efforts manuels. Si ces critères vous importent, recherchez des solutions qui offrent cette fonctionnalité.

☐ Comment la solution est-elle utilisée par les auditeurs ?

Les auditeurs internes et tiers exigent un accès aux données de gestion des vulnérabilités pour mener à bien leur mission. Intéressez-vous à des solutions qui vous permettent de fournir un accès aux fonctionnalités de gestion de la conformité aux auditeurs.

☐ La solution opère-t-elle une ségrégation des actifs à des fins de conformité ?

La plupart des lois et réglementations relatives à la sécurité du réseau mettent en avant un sous-ensemble d'actifs, notamment l'obligation faite par la réglementation Sarbanes-Oxley de protéger uniquement les systèmes utilisés pour le reporting financier, ou bien la réglementation PCI concernant la protection des seuls systèmes utilisés pour traiter ou transmettre les données du détenteur de la carte de règlement. Assurez-vous que votre solution de gestion des vulnérabilités vous permet d'affecter des actifs spécifiques à des groupes associés à des exigences spécifiques en matière de politiques.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Quels sont les contrôles et politiques pris en charge par la solution ?

Les contrôles sont créés d'après les normes CIS et NIST et sont mappés vers des infrastructures et des réglementations telles que COBIT, ISO et ITIL. Les contrôles sont au cœur des politiques de conformité, ces dernières étant des ensembles de contrôles ayant trait à une ou plusieurs technologies déployées dans votre environnement. Chaque contrôle de la politique comprend une instruction sur la manière dont un élément propre à une technologie doit être déployé ainsi qu'une ou plusieurs vérifications réalisées par la solution pour valider le contrôle. Intéressez-vous à une solution qui prend en charge tous ces facteurs.

☐ La solution peut-elle supporter des politiques existantes ?

Vérifiez que la solution de gestion des vulnérabilités que vous sélectionnerez comprend une bibliothèque de politiques avec des contrôles que vous pouvez directement importer dans votre compte et utiliser pour le reporting sur la conformité. Les contrôles doivent être classés par technologie, infrastructure ou réglementation de conformité et par type de vérification de la conformité. Une fois importés, les contrôles doivent pouvoir être édités pour ajuster les valeurs et les technologies de contrôle et répondre ainsi au mieux aux besoins de votre entreprise.

☐ Comment la solution fournit-elle un journal d'audit protégé ?

Les auditeurs soupçonneront (et rejetteront probablement) toute donnée de vulnérabilités qui peut être manipulée par votre entreprise. Assurez-vous que la solution ne permet pas aux utilisateurs d'avoir directement accès aux données de vulnérabilités autrement qu'en mode lecture seule. Veillez à vérifier à 100% que les données de vulnérabilités de votre entreprise sont totalement protégées – et isolées – contre toute manipulation externe.

Gestion

☐ Comment la solution vous permet-elle de gérer les actifs ?

Le regroupement des actifs permet d'organiser des actifs par groupes et entités en leur affectant notamment des niveaux d'impact. Cette fonctionnalité est critique pour la solution que vous choisirez. Assurez-vous que la solution offre une grande souplesse et une précision granulaire pour l'analyse, la remédiation et le reporting des vulnérabilités.

☐ Comment la solution vous permet-elle de gérer les utilisateurs ?

Le processus de gestion des utilisateurs de la solution de VM affecte essentiellement différents niveaux de droits d'accès à base de profil. Ces niveaux permettent d'établir des cartes des équipements, de réaliser des analyses de vulnérabilité, de créer des politiques, de gérer la remédiation et également d'administrer la conformité des politiques. Assurez-vous de la puissance de la solution et qu'elle vous permet de gérer les utilisateurs (de manière détaillée et granulaire) efficacement.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Comment la solution fonctionne-t-elle avec des configurations réseau complexes ?

En informatique, la complexité ralentit souvent le traitement et retarde l'exécution d'opérations pourtant simples. Testez les fonctionnalités de gestion des actifs et des personnes de la solution de VM. Vérifiez que la solution facilite la segmentation de votre réseau pour garantir une gestion des vulnérabilités à la fois efficace et précise.

☐ Faut-il prévoir de la maintenance système, notamment patcher le logiciel d'analyse ?

La solution de gestion des vulnérabilités que vous choisirez peut alourdir - ou non - vos contraintes permanentes de corriger les logiciels. Mettez-vous en quête de solutions SaaS. En effet, ces dernières utilisent une plate-forme à la demande et gèrent automatiquement toutes les mises à jour de patch et système. Assurez-vous qu'il ne vous faut rien télécharger, installer, mettre à jour ou maintenir… même sur les sondes internes. Chaque fois que vous utilisez votre solution de gestion des vulnérabilités, vous devez avoir la certitude de disposer de la toute dernière version.

☐ Quelles sont les actions imposées par les auditeurs pour gérer l'activité ?

Les exigences d'une équipe d'audit peuvent être contraignantes. La solution de gestion des vulnérabilités que vous choisirez doit permettre à un Manager ou à un responsable d'une unité de créer en toute simplicité des comptes utilisateurs destinés aux personnes autorisées à réaliser un audit. Même si vous ne souhaitez probablement pas que les auditeurs puissent lancer des analyses de conformité, ces derniers doivent pouvoir définir des politiques et exécuter des rapports d'après des données d'analyse de la conformité.

Coûts

☐ Quels sont les coûts de la gestion des vulnérabilités avec des solutions logicielles classiques ?

Appréhendez l'ensemble des coûts des différentes solutions de gestion des vulnérabilités que vous évaluez. Assurez-vous de bien calculer le véritable coût total de possession. L'utilisation d'une solution de gestion des vulnérabilités logicielle entraîne de nombreux coûts : le logiciel en lui-même exige une licence, ainsi que des frais annuels pour le support et la maintenance. De plus, les utilisateurs et les administrateurs devront suivre une formation. Sans oublier le processus qui mobilise beaucoup de personnes pour obtenir les approbations au niveau des différents services, et aussi pour configurer et optimiser les applications. La maintenance et le partitionnement d'une base de données sont également indispensables, ainsi que le chiffrement pour sécuriser les données. Prendre en charge et maintenir les applications nécessite du personnel pour tester et installer des mises à jour et de nouvelles signatures, ainsi que pour effectuer des analyses et la remédiation. Sans oublier le coût des serveurs, des appliances, de l'infrastructure de stockage et de la reprise après incident.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ N'est-il pas plus rentable de faire appel à un consultant ?

Un consultant peut être d'une aide précieuse, mais sa mission se concentre généralement sur un test de pénétration qui se contente de trouver les vulnérabilités à un moment donné. Payer un consultant pour procéder à des évaluations des vulnérabilités régulières et permanentes devient rapidement trop coûteux par rapport à d'autres solutions. Un consultant peut surtout vous servir à enrichir l'expertise du service chargé de la sécurité et vous aider à remédier les problèmes qui ne sont pas pris en charge par le processus de gestion des vulnérabilités.

☐ Ferais-je des économies si j'utilisais un logiciel Open Source gratuit ?

Il peut être tentant d'utiliser un logiciel Open Source gratuit, mais à long terme, vous devez calculer les coûts réels et la rentabilité globale d'un tel choix. Les inconvénients évidents tels qu'une qualité de code douteuse, l'injection potentielle de vulnérabilités via des modules Open Source non testés ainsi qu'une formation et un support insuffisants doivent peser lourd dans votre décision. En outre, vous devez évidemment continuer à assumer les traditionnels coûts d'utilisation des logiciels mentionnés plus haut.

☐ Un logiciel de gestion des vulnérabilités commercial est-il plus rentable ?

Les logiciels commerciaux seront probablement de meilleure qualité que les solutions Open Source et ils offrent une formation et un support supérieurs. Mais il faut également tenir compte des coûts annuels supplémentaires liés aux licences, au support annuel et à la maintenance. Sans oublier d'assumer les traditionnels coûts d'utilisation des logiciels mentionnés plus haut.

☐ Comment un logiciel fourni sous la forme de service (SaaS) réduit-il les coûts de la gestion des vulnérabilités ?

Un logiciel fourni sous la forme de service (SaaS) est la solution la plus rentable pour la gestion des vulnérabilités. Avec une solution SaaS, un tiers tel que QualysGuard exécute l'application sur un serveur Web Internet sécurisé, que les clients utilisent et contrôlent à la demande à l'aide d'un navigateur Web. Vous vous acquittez d'un abonnement périodique plutôt que de payer pour un logiciel, des mises à jour régulières et une maintenance permanente qui vous permet d'économiser de l'argent.

☐ Du point de vue opérationnel, quelles autres économies une solution SaaS vous permet-elle de faire ?

Une offre SaaS telle que QualysGuard est tout de suite « prête à l'emploi ». Elle se déploie immédiatement, quelle que soit la taille ou la complexité de l'infrastructure. Il n'y a aucun agent à installer ou autres logiciels à déployer où que ce soit sur l'infrastructure. QualysGuard fournit également une API pour une intégration simple et rapide aux plates-formes d'administration de réseaux d'entreprise.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Hormis les économies réalisées sur le déploiement, une solution SaaS n'est-elle pas aussi onéreuse que d'utiliser un logiciel ?

Une solution SaaS comme QualysGuard offre une rentabilité supérieure à un logiciel dans la mesure où il s'agit d'une solution hébergée. En effet, les mises à jour du logiciel et des signatures de vulnérabilités sont automatiques et instantanées pour l'ensemble de l'entreprise. La comparaison des données liées aux vulnérabilités est automatique. Vous obtenez ainsi des vues de l'état de votre sécurité à l'échelle de l'entreprise et instantanées.

☐ Quels sont les coûts difficilement identifiables qu'une solution SaaS permet de réduire ?

Il est possible de réaliser des économies supplémentaires dans de nombreux domaines. Le déploiement de logiciels vers des représentations distribuées à travers un pays ou dans le monde entier nécessite souvent de l'aide sur site ou des services professionnels tandis que le déploiement de la solution SaaS est instantané. Adapter un logiciel nécessite davantage d'infrastructure matérielle. La solution SaaS s'adapte instantanément et infiniment sans exiger le déploiement de matériel supplémentaire. La conformité à la politique de chiffrement de l'entreprise à l'aide d'un logiciel peut s'avérer complexe. Avec l'offre SaaS, le chiffrement est automatique. L'interopérabilité des solutions logicielles exige souvent une personnalisation poussée. L'API XML intégrée de QualysGuard se connecte immédiatement à toute application à l'aide de cette norme universelle.

Fournisseur de solutions

☐ Quels sont l'historique commercial et la pénétration du marché du fournisseur de solutions ?

Assurez-vous que vous sélectionnez un chef de file du marché spécialisé dans la gestion des vulnérabilités. Consultez les ressources d'analystes tels que Gartner et Forrester pour vous informer sur ce qu'ils disent de cette société et de sa solution. Lisez des études de cas et passez leurs références en revue. La société doit avoir une solide réputation et une expérience éprouvée.

☐ Quelle est la gamme de produits de gestion des vulnérabilités du fournisseur de solutions ?

Un fournisseur spécialisé dans les solutions de gestion des vulnérabilités peut généralement offrir un large et riche éventail de produits. Vérifiez que la solution correspond à votre besoin spécifique. En d'autres termes, assurez-vous que la solution est évolutive, assez puissante et également conviviale et économique.

☐ Qui sont les clients du fournisseur de solutions ?

Informez-vous sur le nombre de clients qui utilisent la solution … et sur ce qu'ils en disent. Ce fournisseur met-il facilement à disposition des études de cas et des témoignages clients de leaders du marché renommés qui utilisent sa solution ? Ces entreprises utilisent-elles vraiment la solution de gestion des vulnérabilités ? Vérifiez les références et demandez à parler à des clients présents sur votre marché.

Copyright © 2009, Qualys, Inc. Tous droits réservés.

☐ Qui sont les partenaires du fournisseur de solutions ?

Avec qui l'entreprise travaille-t-elle ? Avec quels autres produits sa solution s'intègre-t-elle ? Vérifiez si la solution s'intègre avec des solutions et des technologies de sécurité de pointe dans les domaines de la *Gestion des Informations & des événements de sécurité* (ArcSight, Cisco, netForensics, Network Intelligence, Novell, StillSecure, 1Labs, Symantec), de la *gestion des patches* (Citadel), des *systèmes de gestion des tickets de Help Desk* (CA Service Center, BMC Magic Service Desk, HP Service Desk, Bugzilla et autres), de la *gestion des risques* (Redseal, Skybox), du *contrôle d'accès au réseau* (MetaInfo), des *systèmes IDS/IPS* (Neon Software, ForeScout), des *correctifs réseau* (BlueLane), de l'*analyse du comportement du réseau* (Mazu Networks), de la *gestion des politiques de sécurité* (Archer Technologies, McAfee) et des *tests de pénétration* (Core Security Technologies).

☐ Quelles sont les récompenses récemment obtenues par le fournisseur pour sa solution ?

Les récompenses récentes sont un autre indicateur majeur de la qualité du produit et de sa pénétration du marché. Par exemple, parmi les récentes récompenses décernées à Qualys figurent SC Magazine Awards 2008 Winner (U.S.), Information Security Readers Choice 2008, Frost & Sullivan Best Practices Award 2008, Information Security Decisions Best in Show 2007, SC Magazine Awards 2007 Europe Winner et Network World Clear Choice Award.

☐ Puis-je obtenir une version d'évaluation gratuite de la solution de gestion des vulnérabilités ?

Si vous ne pouvez pas essayer une solution, ne l'achetez pas. Vous devez pouvoir vérifier si la solution fonctionne dans votre environnement et la tester pleinement. Il est important de vérifier combien il est facile (ou difficile) de l'installer, de la maintenir et de l'utiliser dans l'ensemble de votre entreprise.

Qualys vous propose une version d'évaluation gratuite de 14 jours de la solution QualysGuard pleinement fonctionnelle. Commencez votre évaluation dès maintenant en vous connectant sur : http://www.qualys.com/products/trials/.

Copyright © 2009, Qualys, Inc. Tous droits réservés.